Refine Search

Search Results -

Terms	Documents
L19 and L17	2

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search: L20

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Thursday, April 28, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR			
L20	L19 and l17	2	L20
L19	L18 and @ad<=19980414	2	L19
L18	L16 and (tag$ or label$)	19	L18
L17	L16 and @ad<=19980414	2	L17
L16	L15 and tag$	19	L16
L15	L13 and (crypto$ or encrypt$ or decrypt$)	77	L15
L14	L13 and (electronic$ near2 tag$)	0	L14
L13	"zero knowledge protocol" and authenticat$	80	L13
DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L12	L11 and zero$	2	L12
L11	5546463.pn. or 5303370.pn. or 6363483.pn. or 6069955.pn. or 5878142.pn. or 5666417.pn. or 5640002.pn. or 5574790.pn.	8	L11

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR

L10	L9 and modular$	15	L10
L9	L8 and ((self$ or automatic$) with dispens$)	60	L9
L8	(parabol$ with (shape or form$)) and @ad<=20011222	14073	L8
L7	L6 and parabol$	2	L7
L6	L5 and ((self$ or automatic$) with dispens$)	60	L6
L5	L2 and @ad<=20011222	237	L5
L4	L3 and l2	3	L4
L3	221/9,13.ccls.	961	L3
L2	L1 and (work adj station) and hous$	416	L2
L1	dispens$ and display$	67109	L1

END OF SEARCH HISTORY

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 2 of 2 returned.

☐ 1. Document ID: US 6434238 B1

Using default format because multiple data bases are involved.

L17: Entry 1 of 2 File: USPT Aug 13, 2002

US-PAT-NO: 6434238
DOCUMENT-IDENTIFIER: US 6434238 B1
**** See image for Certificate of Correction ****

TITLE: Multi-purpose transaction card system

DATE-ISSUED: August 13, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chaum; David	Sherman Oaks	CA		
Ferguson; Niels	Amsterdam			NL
Van Der Hoek; Jelte	Amsterdam			NL

US-CL-CURRENT: 380/45; 380/30, 705/67, 713/172

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. De

☐ 2. Document ID: US 5297206 A

L17: Entry 2 of 2 File: USPT Mar 22, 1994

US-PAT-NO: 5297206
DOCUMENT-IDENTIFIER: US 5297206 A

TITLE: Cryptographic method for communication and electronic signatures

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L16 and @ad<=19980414	2

Display Format: - Change Format

Previous Page Next Page Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Generate Collection Print

cite

L17: Entry 1 of 2 File: USPT Aug 13, 2002

US-PAT-NO: 6434238
DOCUMENT-IDENTIFIER: US 6434238 B1
** See image for Certificate of Correction **

no tag label

TITLE: Multi-purpose transaction card system

DATE-ISSUED: August 13, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chaum; David	Sherman Oaks	CA		
Ferguson; Niels	Amsterdam			NL
Van Der Hoek; Jelte	Amsterdam			NL

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
InfoSpace, Inc.	Bellevue	WA			02

APPL-NO: 08/ 909480 [PALM]
DATE FILED: August 11, 1997

PARENT-CASE:
This application is a continuation (under 35 USC.sctn.120/365) of PCT/US95/01765 designating the U.S. and filed Feb. 13, 1995 as, in turn, a continuation-in-part (under 35 .sctn. 120/365) of U.S. application Ser. No. 08/179,962 filed Jan. 11, 1994, now U.S. Pat. No. 5,434,919.

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 380/45; 705/67, 713/172, 380/30
US-CL-CURRENT: 380/45; 380/30, 705/67, 713/172

FIELD-OF-SEARCH: 380/30, 380/45-47, 235/380, 705/67-69, 713/169-172

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3668653	June 1972	Fair et al.	
☐	4625276	November 1986	Benton et al.	

☐	4630201	December 1986	White	
☐	4742546	May 1988	Nishimura	
☐	4747050	May 1988	Brachtl et al.	380/45
☐	4771376	September 1988	Kamiya	
☐	4771461	September 1988	Matyas	
☐	4877947	October 1989	Mori	
☐	4881264	November 1989	Merkle	
☐	4885777	December 1989	Takaragi et al.	
☐	4906828	March 1990	Halpern	
☐	4914698	April 1990	Chaum	
☐	4935962	June 1990	Austin	
☐	4947430	August 1990	Chaum	
☐	4987593	January 1991	Chaum	
☐	5005200	April 1991	Fischer	
☐	5016009	May 1991	Whiting et al.	
☐	5016274	May 1991	Micali et al.	
☐	5034597	July 1991	Atsumi et al.	
☐	5117458	May 1992	Takaragi et al.	
☐	5131039	July 1992	Chaum	
☐	5140634	August 1992	Guillou et al.	
☐	5212788	May 1993	Lomet el al.	
☐	5214702	May 1993	Fischer	
☐	5220501	June 1993	Lawlor et al.	
☐	5221838	June 1993	Gutman et al.	
☐	5241599	August 1993	Bellovin et al.	
☐	5247578	September 1993	Pailles et al.	
☐	5267314	November 1993	Stambler	
☐	5280527	January 1994	Gullman et al.	
☐	5299263	March 1994	Beller et al.	
☐	5311594	May 1994	Penzias	
☐	5361267	November 1994	Godiwala et al.	
☐	5373558	December 1994	Chaum	
☐	5402490	March 1995	Mihm, Jr.	
☐	5434919	July 1995	Chaum	380/30
☐	5748737	May 1998	Daggar	235/380

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 281 224	September 1988	EP	
0 291 834	November 1988	EP	
0 421 808	April 1991	EP	
0439847	August 1991	EP	
0 535 863	April 1993	EP	
0 573 245	December 1993	EP	
2 274 523	July 1994	GB	
WO 89/08957	September 1989	WO	
WO 90/04892	May 1990	WO	

OTHER PUBLICATIONS

Chaum et al, "Untraceable Electronic Cash", Advances in Cyptology--Cryto '88, pp. 319-327.
Even et al, "On-line/Off-line Digital Signatures", Advances in Cryptology--Crypto '89, pp. 263-275.
Box et al, SmartCash: A Practical Electronic Payment System, CWI Technical Report CS-R9035.
Diffie et al, New Directions in Cyrptography, IEEE Transactions on Information Theory, vol. IT22, No. 6, No. 79, pp. 644-654.
Lamport, "Construction Digital Signatures form a One Way Function", SRI Technical Report CSL-08.
"Matrix Digital Signature for Use With the Date Encryption Algorithm", IBM Technical Disclosure Bulletin, vol. 28, No. 2, Jul. 1985, pp. 603-604.
Merkle, "A Digital Signature Based on a Conventional Encryption Function", Advances in Cryptology--Crypto '87, pp. 369-378.
Chaum et al, "Undeniable Signatures", Advances in Crytology--Crypto '89, pp. 212-216.

ART-UNIT: 2661

PRIMARY-EXAMINER: Cangialosi; Salvatore

ABSTRACT:

Disclosed is a multi-purpose transaction card system comprising an issuer, one or more cards, one or more terminals, and optionally one or more acquires, communicating using a variety of cryptographic confidentiality and authentication methods. Cards authenticate messages using public key based cryptographic without themselves performing the extensive computations usually associated with such cryptography. Integrity of complex transaction sequences and plural card storage updates are maintained, even under intentionally generated interruptions and/or modifications of data transmitted between card and terminal. Cards do not reveal any information to the terminal which is not directly necessary for the transaction or any information to which the terminal should not have access, though externally measurable aspects of its behavior. Transaction types supported include those suitable for off-line credit cards, in which the "open to buy" is maintained on the card.

10 Claims, 58 Drawing figures

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Cite

End of Result Set

Generate Collection Print

no tag/lab

L17: Entry 2 of 2 File: USPT Mar 22, 1994

US-PAT-NO: 5297206
DOCUMENT-IDENTIFIER: US 5297206 A

TITLE: Cryptographic method for communication and electronic signatures

DATE-ISSUED: March 22, 1994

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Orton; Glenn A.	Hamilton, Ont.			CA

APPL-NO: 07/ 957105 [PALM]
DATE FILED: October 7, 1992

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATION This application is a continuation-in-part of my earlier filed U.S. patent application Ser. No. 07/854,389 filed Mar. 19, 1992 and now abandoned.

INT-CL: [05] H04L 9/30, H04L 9/32

US-CL-ISSUED: 380/30; 380/23, 380/28
US-CL-CURRENT: 380/30; 380/28, 713/174, 713/180

FIELD-OF-SEARCH: 380/30, 380/23-25, 380/28

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4306111	December 1981	Lu et al.	380/30
☐	4399323	August 1983	Henry	380/30
☐	4633036	December 1986	Hellman et al.	380/30
☐	4748668	May 1988	Shamir et al.	380/30 X
☐	4995082	February 1991	Schnorr	380/30 X
☐	5016274	May 1991	Micali et al.	380/30 X
☐	5054066	October 1991	Rick et al.	380/30
	5073935	December 1991	Pastur	380/30

☐

☐ 5097504 March 1992 Camion et al. 380/30 X

ART-UNIT: 222

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Hicks; Richard J.

ABSTRACT:

A cryptographic method for communication and electronic signatures is described. The system includes at least one encoding device coupled to at least one decoding device by a communications channel. The method is a form of public-key or two-key cryptosystem, where the private decoding key is not feasibly determinable from the associated public encoding key. A block of ns bits of a message-to-be-transferred M (or key-to-be-distributed) is enciphered to ciphertext by first mapping M to a set {x.sub.1, x.sub.2, . . . , x.sub.n }, where x.sub.i [0, 2.sup.s). Then the ciphertext {y.sub.1, y.sub.2, . . . , y.sub.m } is determined by ##EQU1## mod q.sub.j, for j=1 to m', and ##EQU2## for j=m'+1 to m, where ##EQU3## The encoding key (associated with the intended receiver) consists of integers a.sub.ij, g.sub.j, and positive fractions f.sub.i, for i=1 to n and for j=1 to m, and positive integers q.sub.j, for j=1 to m'. The ciphertext is deciphered (with a secret key known only to the intended receiver) by solving a knapsack ##EQU4## with secret superincreasing weights {b.sub.1, b.sub.2, . . . , b.sub.n } and target value b.ident..vertline.w.sup.-1 .vertline.w'.sup.-1 y.vertline..sub.Q .vertline..sub.P, where y.ident.{y.sub.1, y.sub.2, . . . , y.sub.m } mod {q.sub.1, q.sub.2, . . . , q.sub.m }, ##EQU5## and w, w', and {q.sub.m'+1, q.sub.m'+2, . . . , q.sub.m } are secret integers. The resulting terms {x'.sub.1, x'.sub.2, . . . , x'.sub.n } correspond to the original message terms {x.sub.1, x.sub.2, . . . , x.sub.n }.

20 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#